USAWC STRATEGY RESEARCH PROJECT

DISTRIBUTED GENERATION TO COUNTER GRID VULNERABILITY

by

Lieutenant Colonel Anton H. Nerad II
United States Marine Corps

Professor James Kievit
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **30 MAR 2007**	2. REPORT TYPE **Strategy Research Project**	3. DATES COVERED **00-00-2006 to 00-00-2007**
4. TITLE AND SUBTITLE **Distributed Generation to Counter Grid Vulnerability**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Anton Nerad**		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**19**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

ABSTRACT

AUTHOR: Lieutenant Colonel Anton H. Nerad II

TITLE: Distributed Generation to Counter Grid Vulnerability

FORMAT: Strategy Research Project

DATE: 27 March 2007 WORD COUNT: 5548 PAGES: 19

KEY TERMS: Security, Dispersed, Defense

CLASSIFICATION: Unclassified

In this paper I examine how the United States can best defend against the interruption of critical electrical energy by hostile acts, identify and examine some of the vulnerabilities to our nation's power generation and distribution capabilities, outline several terrorist designs for disruption to it and the resulting economic impact, and provide a possible solution with the adoption of a concept of "distributed generation." Further, I demonstrate a national recognition of those vulnerabilities and explain who has been assigned the responsibility to protect these capabilities. By providing examples of terrorist targets and highlighting several vulnerabilities, I elaborate on the benefits of distributing our energy generation resources and discuss the technologies and their availability, risks, and benefits. Lastly, a discussion concerning ways the government can contribute to the distributed energy picture along with several of the means to best implement and expedite this strategy is provided. While the national strategy is to protect from attacks against our energy infrastructure, there needs to be an effort of dispersing generation capabilities in order to protect against the *effects* of power generation disruption.

DISTRIBUTED GENERATION TO COUNTER GRID VULNERABILITY

Electrical energy is a staple of the American way of life. Nearly every activity we perform every day requires some application of electrical energy, even the task of generating electrical energy. Americans rightly expect that electric power will be there when they need it, and have adapted their lives to the plethora of cheap, available, and dependable electric power. Our way of life is sustained by electric power plants and the infrastructure needed to move the electricity from the point of origin to the point of use. This system of tightly coupled, integrated and interdependent systems, however, also is a key vulnerability to our way of life. Our nation's centralized electrical power generation system and its distribution network includes fragilities and vulnerabilities that can be exploited by hostile or even natural acts. A more modern decentralized and distributed electrical power generation model based upon distributed generation of electrical energy is our best defense.

Our country relies heavily upon centralized electrical power generation plants connected to a networked grid to supply our needs. Those needs are high and growing; the typical home uses approximately 24 Kilowatts (kW) and the average McDonald's uses about 500 kW of electricity daily.[1] Our need for electricity is constantly increasing, requiring the United States to import more electricity or build more plants to generate for its generation. In 2005 total electric power consumption in the United States was 29,404,894 megawatts (MW) while total domestic electric production was only 20,365,258 MW, of which 18,532,836 MW was generated using conventional methods and fuels such as coal, oil, gas, and nuclear and another 1,832,422 MW by using renewable energy such as wind, solar, hydro electric, and geo thermal.[2] The remaining 9,039,636 MW, or roughly 31 percent, was imported.

In our current electrical generation and distribution system, electric power moves from large central generating stations to the end consumers via a transmission grid. There are many opportunities for disruption within each of these subsystems, the first being the points of generation where raw materials, such as coal, oil, natural gas, etc., are converted into electric power. Secondly, there are the receiving stations and substations, which are the mechanisms that distribute the electricity to the consumers, such as hospitals, factories, homes, military bases, and schools, to name a few. Lastly, and usually the least obvious but equally critical infrastructures in the process, are the high-tension electrical power lines that transmit the electricity between the generation point and the receiving stations and the pipelines, rail lines, and roadways that brought the fuel to the generation points[3].

The major source of raw material for electricity generation is coal, which provides 49.7 percent of the total fuel used. The remaining raw material total is made up of Nuclear at 19.3

percent, natural gas at 18.7 percent, petroleum at 3 percent, hydroelectric at 6.5 percent, renewable (solar, wind, etc.) at 2.3 percent, other gases and fuels at 0.5 percent.[4] Most of this material is brought to the generation point using railways, pipelines, or ships – creating a transportation extension to the electrical power grid itself. The nation's electrical power system includes 158,000 miles of primary electric transmission lines, 5,000 electrical power plants (totaling 800,000 MW) including 103 nuclear power reactors, 2 million miles of oil pipelines, 1.3 million miles of gas pipelines, 2,000 petroleum terminals, one million gas and oil wells, and 150 oil refineries.[5] The electrical energy industry is a large tightly interconnected web that reaches every corner of the country.[6]

The U.S. electric power system is a tempting target because electric energy is a large part of the U. S. economy and an important ingredient for our culture and way of life.[7] Although our electric energy production, storage, and transportation facilities are dispersed across the United States, the interconnectedness, openness, and centralized locations make our system vulnerable to various forms of terrorist attack. During electrical power outages of any length of time, homes and businesses currently stand to lose not only idle time, but money as well. Today people and businesses have built their worlds around, and are in need of, reliable and uninterruptible sources of electrical energy. In 1978 explosives left by an unknown source left a hole in the Trans Alaskan pipeline which caused a spill of approximately 670,000 gallons of oil. In 2001 Al Qaeda operatives destroyed the World Trade Center and have designs for more attacks against the U. S. economy.

As the World Trade Center was a central, large, local target, our nation's electrical power generation network presents many of the same vulnerabilities. In 2001 a man with a high powered rifle shot a hole in the Trans Alaskan pipeline, causing a spill of over 285,600 gallons and $8 million dollars in lost royalty revenue and taxes and $20 million dollars in clean up costs.[8] In 2003 a single downed power line caused 21 electric power plants to shut down leaving approximately 50 million people in the Northeastern United States without electricity for over 30 hours.[9] In 2006 Hewlett-Packard estimated that a 15-minute electricity outage at only one of their chip manufacturing plants would cost the company $30 million in lost production and recovery services, all while costing the electrical power company little at all.[10] These kinds of losses can devastate a region, not just the company.

The 2003 U. S. blackout lucidly demonstrates the vulnerability to our electrical power grid and the rapidly ensuing negative effects of electrical power loss. It demonstrates that a tightly interconnected electric grid, as in our current system, can be not only its greatest strength but also its biggest weakness. When there is a problem with even a seemingly minor subsystem, in

this case a broken power line, the interconnected grid itself becomes a very large vulnerability.[11] "The Great Blackout of 2003 will go down in history as one more wake-up call for a nation grown weary of them, a vivid demonstration that the most critical technology of modern life – the electricity that powers virtually every aspect of it – is vulnerable to severe disruption, and growing more so by the day."[12] The loss of any major electrical power plant could leave large regions of the country without electricity.[13] Even an imbalance of electrical power on the grid can cause the "fail safe" system to fail, resulting in the loss of electricity to tens of millions of people at once or, even more disrupting, an electrical power plant could burn out.

Terrorist groups such as Al Qaeda have expressed an interest exploiting vulnerabilities and sensitivities at nuclear sites, and Al Qaeda still has operatives at large in the United States.[14] In 2002 Representative Edward J. Markey, a senior member of the House Energy and Commerce Committee, was quoted as saying "the nation's 103 nuclear power reactors are vulnerable to a potentially catastrophic terrorist attack but have taken few safety countermeasures since September 11, 2001 even though they have been targeted by Al Qaeda…" Rep. Markey also said "the nation's commercially operated reactors are at risk from a wide variety of assaults, including sabotage from foreign workers who were not adequately screened…and are also vulnerable to the same kind of suicide hijackings that leveled the World Trade Center and damaged the Pentagon…"[15] There are currently twenty-one nuclear facilities located within a five-mile radius of an airport. Additionally, most nuclear facilities store significant amounts of spent nuclear fuel in non-hardened structures. Rep. Markey also contends that the guards at these facilities are under trained and in some cases incapable of combating an attack on the site from terrorists who want to gain entry.[16] The impact of an attack to a nuclear facility could be devastating to the area.

Since the mid 1990s, security experts have shown concern about attacks on the electrical power gird. In a war game called "Eligible Receiver" in 1997, government hackers showed they could gain access to internal networks at electrical power plants in many of America's cities.[17] Guerrilla movements all over the world have made a specialty of blowing up electrical power pylons. A single isolated bomb on a vital transmission corridor is an easily recoverable event, but coordinated bombs could have a much larger effect.[18] "Security experts have also been saying the electrical grid is vulnerable to deliberate attack, most likely with bombs but also possible through a cyber-assault by hackers, terrorists or enemy nations."[19] Additionally, the Department of Energy states on their website that "Today, we can anticipate facing an adversary with more resources and enhanced capabilities, and who routinely plans to use suicidal tactics as a portion of their overall tactical plan."[20]

More than just the electric generation plants, there are other vulnerabilities, such as major transmission lines, large gas pipelines, the increasing number of larger scale electric plants, and the nation's gradually declining number of oil refineries that need to be considered and discussed.[21] Much attention since September 11, 2001 has been turned toward nuclear power plant security, but virtually little has been done to protect the remaining plants and infrastructure that keeps them running.[22] In 1999 there was a natural gas pipeline explosion in Washington State which spilled 230,000 gallons of natural gas and killed three people and more than 100,000 fish and aquatic life. The explosion destroyed one home, twenty-six acres of trees, and 2.5 miles of vegetation.[23] Strategic pipelines represent one of our largest vulnerabilities, as more than 90 percent of the United States' new electrical power plants burn natural gas as their fuel.[24] A disruption in the natural gas supply, such as one that could occur through a pipeline problem such as a rupture, could result in millions of homes without heat or electricity and thousands of factories and businesses not operating. This would cause major economic problems for the affected region in addition to the environmental problems of rupture.

Oil refineries also pose great risk from attack. While they arguably are easier to protect than a pipeline, they are very expensive to guard. After September 11, for example, Conoco Phillips spent $5 million in security upgrades for only one of its refining facilities.[25] Also of great concern is the dwindling number of refining facilities in the United States. Since the mid 1970s the number of refineries has dwindled from 300 to just 150.[26] These remaining refineries are larger and consequently produce a larger percentage of refined fuel; we saw the adverse effects of just one closure after Hurricane Katrina in 2005.

Today we face terrorists with more resources and capabilities than ever who routinely use suicide attacks as part of their overall modus operandi.[27] The Department of Energy (DOE) has charged the Office of Health, Safety, and Security (HSS) with the protection of America's energy systems, which provides this through a protective force. This protective force uses a tactical response force concept along with an integrated use of security technology and a barrier plan to combat attacks.[28] The tactical response force is an elite force designed to be highly trained and tactically skilled in early detection and assessment of enemy capabilities to allow interdiction as far from the site as possible.[29] They also establish a formidable perimeter and are heavily armed and can maneuver decisively against potential aggressors using lightly armored vehicles with weapons along with units tactically positioned to provide support.[30] Most of this protection, however, goes to nuclear facilities. While the point defense of nuclear facilities or other generating stations is of the utmost importance, it is important to consider the vulnerabilities of the electrical generation and distribution system in its entirety. While the generation plant itself

may be safeguarded and able to generate, the electricity it produces may be interdicted along many points downstream and away from protective forces.

Since September 11, the government has focused its attention to updating security for the nation's nuclear power plants. While Patriot missiles have been placed at Palo Verde nuclear facility in Arizona and Army National Guard troops have been stationed at other nuclear facilities to provide security,[31] very few facilities have the capability to defend against air attacks. In total, only $370 million has been spent on security at the nuclear power plants[32]. Beyond these few nuclear facilities, very little has been done to protect the non-nuclear power generation facilities. Although there is a health risk associated with an attack on a nuclear site, the non-nuclear plants are just as critical to the primary function of providing our nation with electricity. Regions of the country could be blacked out if just one plant of any type is attacked or has a disruption of its fuel delivery. Chuck Gray, executive director of the National Association of Regulatory Utility Commissioners, is quoted as saying: "There is no practical way to protect every mile of the nation's energy system with guns, gates, and guards."[33]

So how can we protect the nation's 158,000 miles of primary electric transmission lines, 2 million miles of oil pipelines, 1.3 million miles of gas pipelines, 2,000 petroleum terminals, one million gas and oil wells, and 150 oil refineries?[34] Currently, the United States can do very little to protect this infrastructure from attack. Although experts have spent a great deal of money and thought as to how to protect the nations 103 nuclear reactors and they are somewhat secure in the post September 11th world, leaders still need to address the concerns of protecting and ensuring the electric power generation needs of our country, which in total creates a very large target indeed for terrorists. It would not take a large attack to disable a large part of the country. In January 2007 a winter storm knocked out electricity to 330,000 homes and businesses in Missouri, 11,000 homes and businesses in New York and 122,000 electric customers in Oklahoma without electricity. Repairs and service restoration took up to one week in many cases.[35] These are acts of nature, but what if they were part of a large scale coordinated terrorist attack? How does a government protect millions of miles of pipeline or the primary transmission lines? Because there are really no good answers to these questions, the answer must lie with a better solution.

Several questions come to mind once we fully understand the U. S. current electrical needs and system. If the United States generates its electric power in large, centralized electric power plants then distributes that electricity along transmission lines, what then is the alternative? Do we really need to protect all components of our electrical grid? Or, do we protect against the effects of disruption of electric power due to damage or outages within the

grid? I think the latter is the answer. The large concern with our grid's makeup today is there are few robust options or buffers when problems within the system arise. What are needed are electric power generating components along the nodes and dispersed throughout the system. The alternative is a process of distributed generation, where future electricity generation requirements are built into point-of-use facilities that would allow our system to survive disruptions in nearly every instance. By making all buildings on military bases, schools, and government buildings, and intended places of refuge during a national crisis (such as churches, stadiums, etc.) self sufficient in electrical energy generation, we will have a robust "defense in depth" against attacks or disruptions anywhere in the system. In other words, when portions of the grid are disrupted, then these select buildings continue to provide power to themselves, and any of their excess power to the remaining operating portions of the grid. The power company, in accordance with procedures, would route the power as required by priorities.

What is distributed generation? Power experts define distributed generation in many ways, but it is best described as "the production or generation near the point of use."[36] There are various parties who differentiate the definition in various details. "Some parties define it with size limitations, others exclude back up generation, and yet others make no distinction between generation connected to the transmission system or the distribution system."[37] Perhaps the best definition is from the California Energy Commission, which

> …assumes the following definition: Distributed generation is electric generation connected to the distribution level of the transmission and distribution grid usually located at or near the intended place of use. While distributed generation is inherently related to local transactions vis-à-vis activities that may otherwise be construed to be in interstate commerce, the definition is not designed to preclude the use of distributed generation at the transmission level if the economics of doing so are warranted.[38]

Distributed generation has many different uses from its most limited potential of personal generators to supplying complete electrical needs[39]. Personal generators usually serve as back-up electrical power, but this is a shortsighted although common and expensive application. Because consumers use personal generators only in emergences, there is a very low return on investment. Agencies can also use distributed generation as an augmentation to current electrical power by providing part of normal electricity needs and selling back any excess electricity to the grid. In this manner, distributed generation could buffer "power spikes," preventing overload to the overall system which can cause automatic shutdowns and costly machine resets. Lastly, and most promising, is to use distributed generation to provide primary electrical power for a facility and the capability to supply excess electrical power into the grid which would provide excess electrical power for use by other customers.[40] Additionally,

engineers can size distributed generation systems to meet a facility's total electrical requirements or they can size the systems to partially replace or supplement electrical service from the grid. Distributed generation systems typically range in size from less than a kilowatt to tens of megawatts, although an individual unit's generating capacity depends on allocable space and size of load.[41]

Distributed generation has many applications, currently the most common being a back up electricity source whenever the normal source of electricity fails. The California Building Standards Code, as an example, requires standby or emergency electrical power systems serve specific types of equipment within specific types of buildings. Electrical loads, which must be served during an electricity failure or interruption, are those that could create a public health and safety hazard or hamper rescue or fire-fighting operations. "Industrial and commercial building owners, farms, and homeowners may also install optional standby generators and uninterruptible power supplies."[42] These distributed generation systems serve electric loads which, if cut off from the normal electrical power supply, could cause discomfort or serious interruption of a highly reliable electrical power quality to electronic equipment that is vulnerable to voltage fluctuations.[43]

Installations may also complement distributed generation equipment with electric storage and switching equipment to provide a seamless transition between the grid and an on-site electrical power supply.[44] Distributed generation customers can use as a primary source of electricity, essentially reducing or even eliminating reliance on the utility for electric service. "When customer sites are remote and not served by the electric grid, distributed generation is a cost-effective alternative for both the electric customer and the utility – to extending the distribution line to serve the new load. Similarly, on-site electrical power supplies provide electric service to very small loads, such as roadside call boxes, more cost effectively than the grid."[45]

Electric transmission can have significant inefficiencies that vary by the length electricity must travel across power lines. The longer the distance the electricity has to travel, the more electricity that is "lost" in the process. Generating electricity at or near the intended point of use requires the generation of less electricity than would otherwise be required.[46] Additionally, other efficiencies are gained when generating electrical power at or near point of use including thermal issues with heat transfer. Excess heat used from the creation of electricity can be used in heating and cooling systems as well as many other industry specific uses.[47] To make distributed generation most effective many installations are using this extra thermal energy to heat, cool, or dehumidify buildings or to run other processes.[48] This is called cogeneration, or combined heat and electrical power, and it increases grid efficiency and lowers economic and

environmental costs.[49] A U.S. bottling company installed a 1.5 MW cogeneration system after 24 electrical power outages in two years that caused costly reset of equipment and spoilage of product. It now generates 70 percent of its electric and 30 percent of its hot water used for sterilization needs. In all, the company is saving $800,000 a year on electricity.[50] The better solution is to use the more ubiquitous and “free” energy that comes from the wind, sun, and other renewable sources, as well as increasing building efficiency. This will also decrease our need for other sources of energy (oil, gas) and lower the cost of electricity. While not exhaustive, what follows are several examples of several different technologies available.

Distributed generation is available using a variety of technologies and can use many different and widely used fuels, such as natural gas, wind, solar, and biomass to create electricity. Currently, natural gas is the most widely used fuel and electricity at this smaller scale is generated the same as in large electric power plants, however, the size of the generator depends on the usage required.[51] Most companies desire to use distributed generation to help cut costs involved with peak hours electricity usage, therefore they generate at least part of their electric needs during the day when electricity is most expensive. Many companies also use the cogeneration method to heat and cool their buildings, thus optimizing their return on investment.[52]

Wind and solar are technologies that are just now becoming more affordable. Both are renewable sources that are in great supply and do not require delivery or raw materials to generate electricity. Nevada engineers are currently building a solar power plant capable of generating 64 MW, the third largest in the world. Although this is a small electrical power plant when compared to the conventional plants, the only fuel required to generate the electricity is sunshine.[53] There is currently research into deriving energy from both visible and infra-red light, which would allow solar plants to work in cloudy conditions. Kansas is also building an alternative electric energy power plant and will provide 20,000 acres and 183 wind turbines to create 250 MW of electric power to the electric companies.[54]

Not all renewable energy projects have to be as large scale as these. I mention them to demonstrate that the technologies are maturing and are gaining investment for large-scale adaptation and conventional use by power companies. There are new technologies that are allowing solar and wind sources to be optimized for small scale, single building use. A company called XsunX has created a transparent solar cell film technology for use in commercial buildings. Buyers can apply this film to the typical glass of commercial buildings and generate electricity.[55] This makes all of the exterior windows of the building solar panels capable of

producing electrical energy for the entire building. A very promising technology and application that does not only provide power for the building, but, adds electric power to the grid.

Biomass, or farm waste, is a fuel that made from the conversion of waste through anaerobic digesters that break down waste into methane, which, when burned, create electricity. This application has very specific uses in the farming industry, however most farmers view this technology as a solution to their waste management problem and not as a solution to an energy problem, but it can be both.[56] Currently, the trends point that in the next few years thousands of dairies, feedlots, hog farms, and poultry operations will install this technology.[57]

There are some striking advantages to dispersing our nations electrical power needs. Buildings containing self-reliant electric power generating capacity would use little or no fossil fuels, thereby reducing our need for both foreign oil and its transport and security. Dispersion could relieve some of the effects from a terrorist attack on the United State energy infrastructure that would have previously caused major power interruptions, saving businesses and the government money, particularly if consumers used renewable energy sources. The technologies exist today to create self sufficient communities or businesses that need very little power they can not create. There are really three viable options for the future of our grid: continue as we currently are, move toward a basic distributed generation model, or move to a more advanced distributed generation model. The following will cover each option in further detail.

The first option is to continue as we always have, building increasingly larger centralized electric power generating plants. These plants would either be natural gas or nuclear powered, or even increasingly include renewable energy sources. The natural gas plants would require infrastructure to be built to deliver the natural gas needed to generate the electricity. Nuclear plants would require provisions for radioactive waste that the reactors will create in the generation process. The nation will also spend increasing amounts of money trying to keep the system as secure as possible. The primary issue, however, is not solved. Any point along the system that is disrupted, leads to a power failure within a large portion of the system.

The second option is to retrofit all government and military buildings and facilities to generate their own electric power while maintaining connection to the electrical power grid. This would provide the building not only with its immediate electrical power needs, but also the surplus of electricity could be transmitted to the grid for use by other electric customers. This would eliminate the need to build more and larger conventional electrical power generation facilities. The buildings could also make wise use of the cogeneration that is possible when the

electricity is created on site, making the best use of the natural materials involved as well as a significant savings to the military or government entity. This option would also provide areas of refuge and command and control during national emergencies, keeping the military and government up and running during emergencies to help care for the people that have been affected. It also shields them from terrorist attacks on the current electrical power generation facilities.

A third, and possibly the most viable option, would be to retrofit all government and military buildings and facilities as in option two while including all new construction projects, both commercial and residential, to incorporate distributed generation technologies. The government could accomplish this only through changes in legislation and changes to building codes to enforce the adaptation of distributed generation. Such action would also require that utility companies buy excess electrical power generated by the consumers. Currently, the majority of the utility industry has not embraced distributed generation out of fears that it will cut into their bottom line and they will lose money.[58] Forward thinking utility companies, however, should see it as a way of providing more electricity to their consumer base without necessarily upgrading or replacing systems, saving them money in the long run. The government currently gives incentives to companies that participate in distributed generation programs.[59] This must continue and extend to the residential side as well. All new construction could also generate electricity with cogeneration in mind, making the most economical and environmental impact. A percentage of the distributed generation electrical power could also come from alternative energy sources. Scientist make great advances on a daily basis in alternative fuel choices and some mix of them could meet the needs of the nation's electricity requirement.

It is my belief that the third option poses the greatest benefit. Many European nations have already started to move to a distributed generation model incorporating as much alternative fuels as possible. In the United Kingdom decentralizing electrical power generation would save them more than $1.7 billion in nuclear capitol investment and reduce gas consumption by as much at 14 percent.[60] The Dutch are also moving toward distributed generation and Iceland is converting to a hydrogen-based economy.[61] In 2003 in downtown San Francisco, a 1.5 million square foot office building was built with a 1.5 megawatt electrical power generation system. It was allowed to interconnect with the downtown grid and is perhaps the biggest downtown connected distributed generation system in the United States.[62]

There are several strategic consequences for the military. During times of a national emergency, if the nation implements a distributed electrical generation system, there would be assured and predictable places of refuge for citizens to go, functional command and control

facilities, hospitals with reliable and persistent electrical power, as well as many other benefits. Having designated installations, such as military bases, sites designated for refuge, schools, and government buildings that provide their own power would mitigate the effects of a blackout or power outage that currently effect large regions. A distributed generation system would also give us greater command and control capabilities and allow more options for responding to crisis. Additionally, having the ability to set up distributed generation anywhere the military deploys would take the concept into the field, so that military operations, either overseas or nationally deployed as part of civil support, would be neither dependant upon local or indigenous sources nor vulnerable to attacks against large and infrastructure-intense centralized electrical generation systems. I recommend that deployable distributed generation systems leverage renewable sources so as to decrease their dependence upon the logistics of transporting fuels, oils, or other perishables, whose own distribution infrastructure could themselves be a vulnerability. This would free up costly fuel transportation costs, which not only include the costs of the fuel and of its transport, but also the costs of security both in manpower, equipment, and dollars.

While the Department of Homeland Security is responsible for efforts to prepare for and mitigate the consequences of terrorist attacks within the United States, the military can expect, and must be prepared, to be called upon in any civil support mission due to terrorist attacks. Imagine the vulnerability of some of our remote military bases that house important radar and communications systems and draw their power from the end of miles of transmission lines from a distant power station, and whose only ability to generate power is from several diesel generators with a relatively short supply of fuel. Dispersing robust electricity generation to military bases leverages the base security and defense plan into the fold of the overall security of the military facilities, therefore ensuring that there is power to the base when the region's grid is disrupted. Additionally, excess electrical power generated from the base could be used "off base" and directed via the functioning grid components to locations that are without power and have an immediate need for it. The greater dispersal of the system, the fewer large, centralized nodes there are whose damage would have large effects. By dispersing the generation and distribution of electricity, security becomes a local policing issue, and destruction of any one component of the system would not have the same consequences to respond too as the destruction of several major components of our current system.

The policy of solving our future energy requirements by building single point power plants and distributing the power through lines of communication does nothing to reverse the trend of our continual improvement upon and expansion of an electrical grid that is vulnerable by nature,

and during periods of trouble, will affect an indeterminate number of users with unpredictable and unspecified results. I recommend the initiation of a government sponsored, sanctioned, and directed plan to equip all new buildings with their own power generation requirements, preferably that require renewable sources that are not dependent upon a transportation network, and hooked into the grid to provide power back into the grid or draw from it when necessary. Further, the power companies should manage the grid on a precedence of power in the event of an emergency determined in coordination with the Departments of Homeland Security and Defense. It is important that the Department of Defense shift to a distributed generation model, not only to co-locate generation and usage with the current base defense infrastructure and plan, but also to ensure electrical power remains available regardless of the region's infrastructure so that they can continue operations unimpeded by the lack of electrical power. Again, I think the efficiencies of cogeneration should be maximized, and that renewable sources, or sources that require a minimum of logistic support be applied, both for static military base use and for deployable electrical generation requirements.

Electricity is a staple of the American way of life whose demand continues to increase along with the requirement to increase our capacity for its generation. Our culture is also dependant upon electricity, and its interruption rapidly affects our lives, economy, and security. Our electrical generation system in its current construct is far too vulnerable, requiring too much critical infrastructure over too large of an area to protect, while leaving the consequences of an attack unpredictable in terms locations, time to restore power, facilities that will be effected, and specific services that will be available. Continuing to sustain and expand the system in its current conceptual design only complicates its continued security in the future. This nation should embrace a strategy of distributed generation in order to mitigate the effects of attack, reduce the number of nodes whose disruption would have larges consequences, and reduce the risk to our power supply due to attacks on our transportation network.

Endnotes

[1] Richard Munson, "Yes, in My Backyard: Distributed Electric Power," *Issues in Science and Technology* (Winter 2006): 49[database on-line]; available from ProQuest; accessed 5 December 2006.

[2] Energy Information Administration Page, available from http://www.eia.doe.gov/emeu /mer/overview.html; Internet, accessed 11 January 2007.

[3] Ibid.

[4] Ibid.

[5] Matthew Brown, “Energy: Vital but vulnerable,” *State Legislatures* Denver (October/November2003): 12[database on-line]; available from ProQuest; accessed 5 December 2006.

[6] Ibid.

[7] Ibid.

[8] Pacific Northwest Pollution Prevention Resource Center, available from http://www.pprc.org/pubs/newsletter/news0302.html; Internet; Accessed 15 December 2006.

[9] Greg Botelho, “Power returns to most areas hit by blackout,” 15 August 2003; available from https://www.cnn.com/2003/us/08/15/power.outage/index.html; Internet; accessed 22 February 2007.

[10] Munson.

[11] Justin Gillis, “Power Grid More Vulnerable Daily; Inherent Weaknesses of a Reliable Structure Are Now Exposed; [Final Edition],” *The Washington Post* (17 August 2003): A. 14[database on-line]; available from ProQuest; accessed 5 December 2006.

[12] Ibid.

[13] Brown.

[14] Josh Meyer, “The Nation; Nuclear Plants Said to Face Big Attack Risk; [Home edition],” *Los Angeles Times* (26 March 2002): A. 1[database on-line]; available from ProQuest; accessed 5 December 2006.

[15] Ibid.

[16] Ibid.

[17] Gillis.

[18] Ibid.

[19] Ibid.

[20] Office of Policy, linked from Department of Energy Office of Health, Safety and Security Home page at “Mission and Functions” available from http://www.hss.energy.gov/SecPolicy; Internet; accessed 11 January 2007.

[21] Gillis.

[22] Brown.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Protective and Tactical Response Force Policy Frequently Asked Questions, linked from Department of Energy Office of Health, Safety and Security Home page at “Protective Force FAQ” available from http://www.hss.energy.gov/ SecPolicy; Internet; accessed 11 January 2007.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Brown.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Botelho.

[36] California Energy Commission, “Distributed Generation Strategic Plan,” available at http://www.energy.ca.gov/reports/2002-06-12_700-20-002.pdf; Internet; accessed 14 December 2006.

[37] Ibid.

[38] Ibid.

[39] Steve Blankinship, “Study Shows Big Untapped DE Residential Market,” *Power Engineering* (November 2004): 170[database on-line]; available from ProQuest; accessed 5 December 2006.

[40] California Energy Commission.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Munson.

[47] Ibid.

[48] Steve Blankinship, “Distributed generation: DGene is out of the Bottle,” *Power Engineering* (March 2003): 26[database on-line]; available from ProQuest; accessed 5 December 2006.

[49] Munson.

[50] Nicholas Lenssen, “Distributed energy: Finding its niche,” Electric Perspectives (July/August 2003): 36[database on-line]; available from ProQuest; accessed 5 December 2006.

[51] Ibid.

[52] Ibid.

[53] Nevada Solar One Wikipedia page, available from http://en.wikipedia.org/wiki/Nevada_ Solar_One; accessed 7 January 2007.

[54] Sam Hartle, “To address future energy needs, BPU reaches for the sky,” The Kansas City Kansan, 5 January 2007[newspaper on-line]; available from http://www.kansascitykansan.com/articles/2007/01/06/news/news1.txt; Internet; accessed 7 January 2007.

[55] Homeland security and Energy Independence Issues addressed by Solar Technology Page; available from http://www.przoom.com/news/1091; Internet; accessed 7 January 2007.

[56] Lenssen.

[57] Ibid.

[58] Blankinship, Distributed generation: DGene is out of the Bottle.

[59] Lenssen.

[60] “London Betting on Distributed Energy,” ENR (17 April 2006): 14[database on-line]; available from ProQuest; accessed 5 December 2006.

[61] Munson.

[62] Blankinship, Distributed generation: DGene is out of the Bottle.